California ISO

NREL Smart Grid Education Series

The Role of Software-Defined Networking and WAN Virtualization in Securing SCADA Systems

An Alternative to PKI and VPNs for Securing Telemetry Data

April 27, 2016

Thomas (Tom) Williams, Security Architect Lead, California Independent System Operator (ISO)

Overview

SCADA networks provide remote control for critical infrastructure.

Current SCADA security solutions tend to scale poorly and expensively.

In order to scale Smart Grid communication, we need innovation in the security architecture. Do this:

- Securely;
- At reasonable cost;
- Over wide areas.

Background

FERC Order No. 888 asserts the advantages of creating competition in wholesale electricity markets through the creation of independent organizations to operate transmission systems.

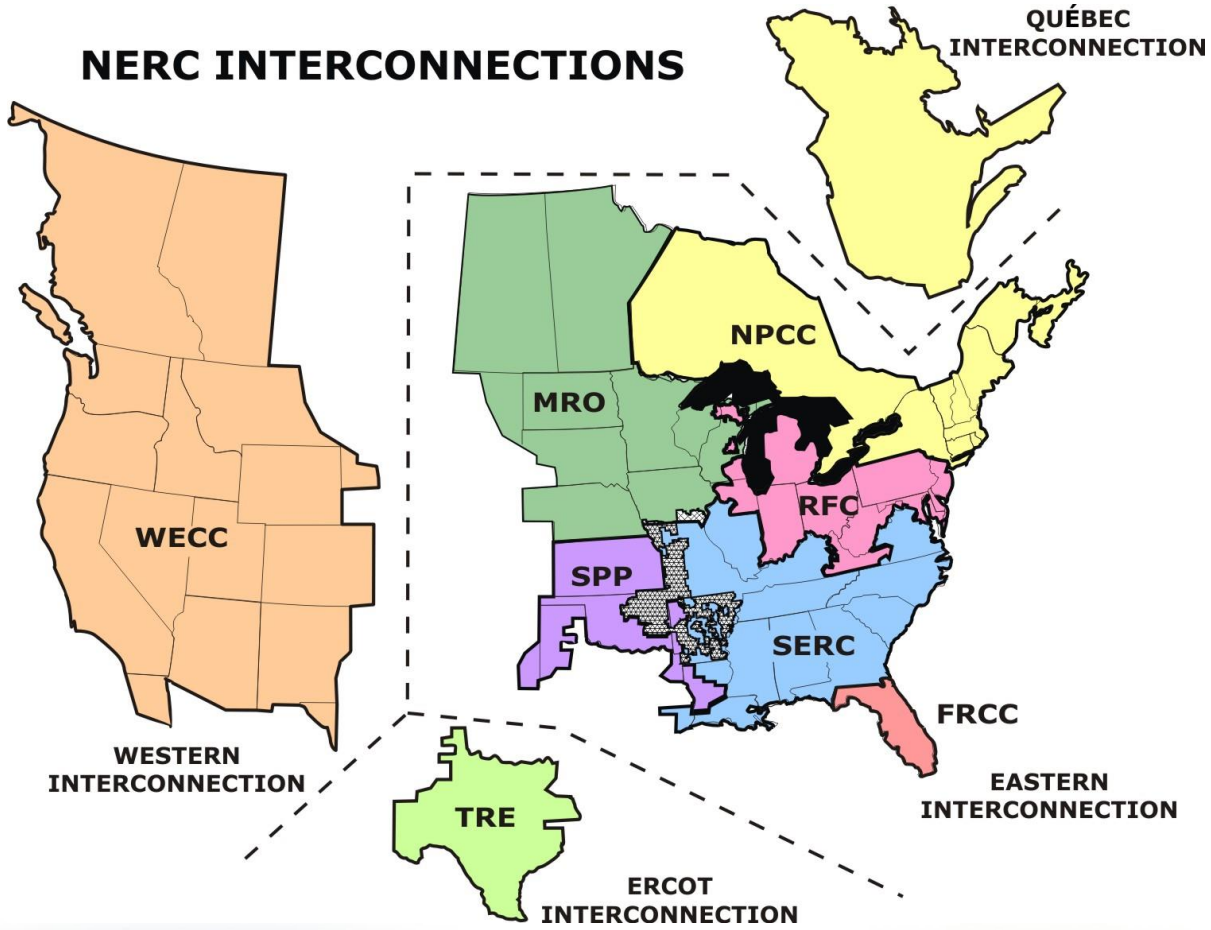
Following this order, North American ISOs and RTOs formed as control areas with responsibility to provide frequency regulation within an Interconnection.

ISOs and RTOs function as “nerve centers” controlling electricity flow within a control area.

NERC Interconnections

NERC is under oversight of FERC and Canadian governmental authorities.

An interconnection is a wide-area synchronous system.



Frequency Regulation / Control

SCADA systems directly control generation to adjust power output in response to load.

The generation equipment automatically responds to SCADA signals in real time.

A prescribed level of grid frequency assures the reliability and safety of the system as a whole.

Security Requirements

What needs to be secured:

- SCADA signals.

Why SCADA signals need to be secured:

- To protect against unauthorized signals to change system frequency.

How SCADA signals need to be secured:

- Protect signals from unauthorized modification and delivery denial.

Security Challenges

SCADA protocols are open.

Security problems magnify in IP networks.

We need a new security architecture to solve a problem resulting from deregulation:

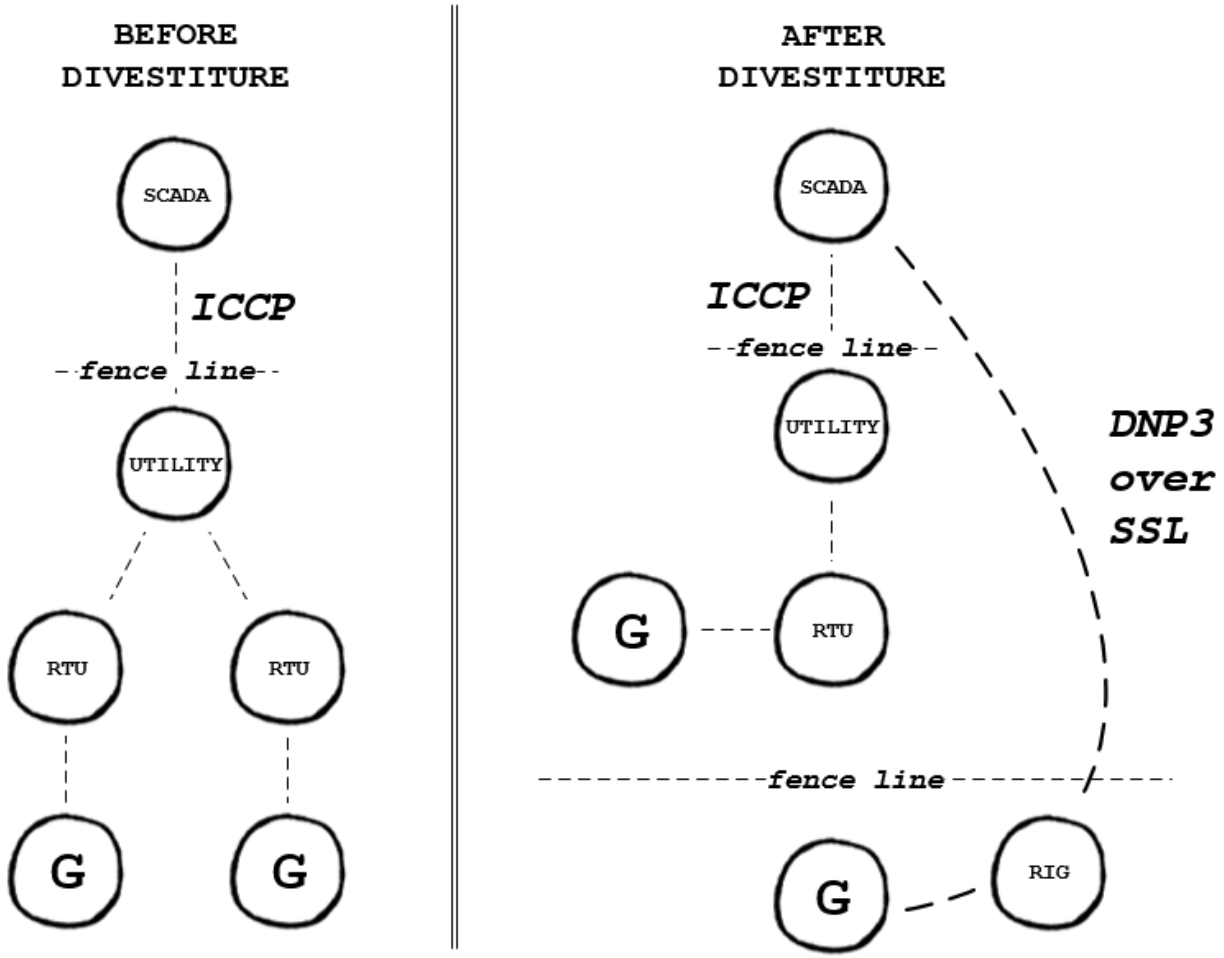
- *Divested generator assets severed from ISO SCADA systems.*

Deregulation

Assumed:

- Competitive markets thrive with lots of participants.
- Deregulation mitigates market power.

Utilities were required to divest some of their generation assets.



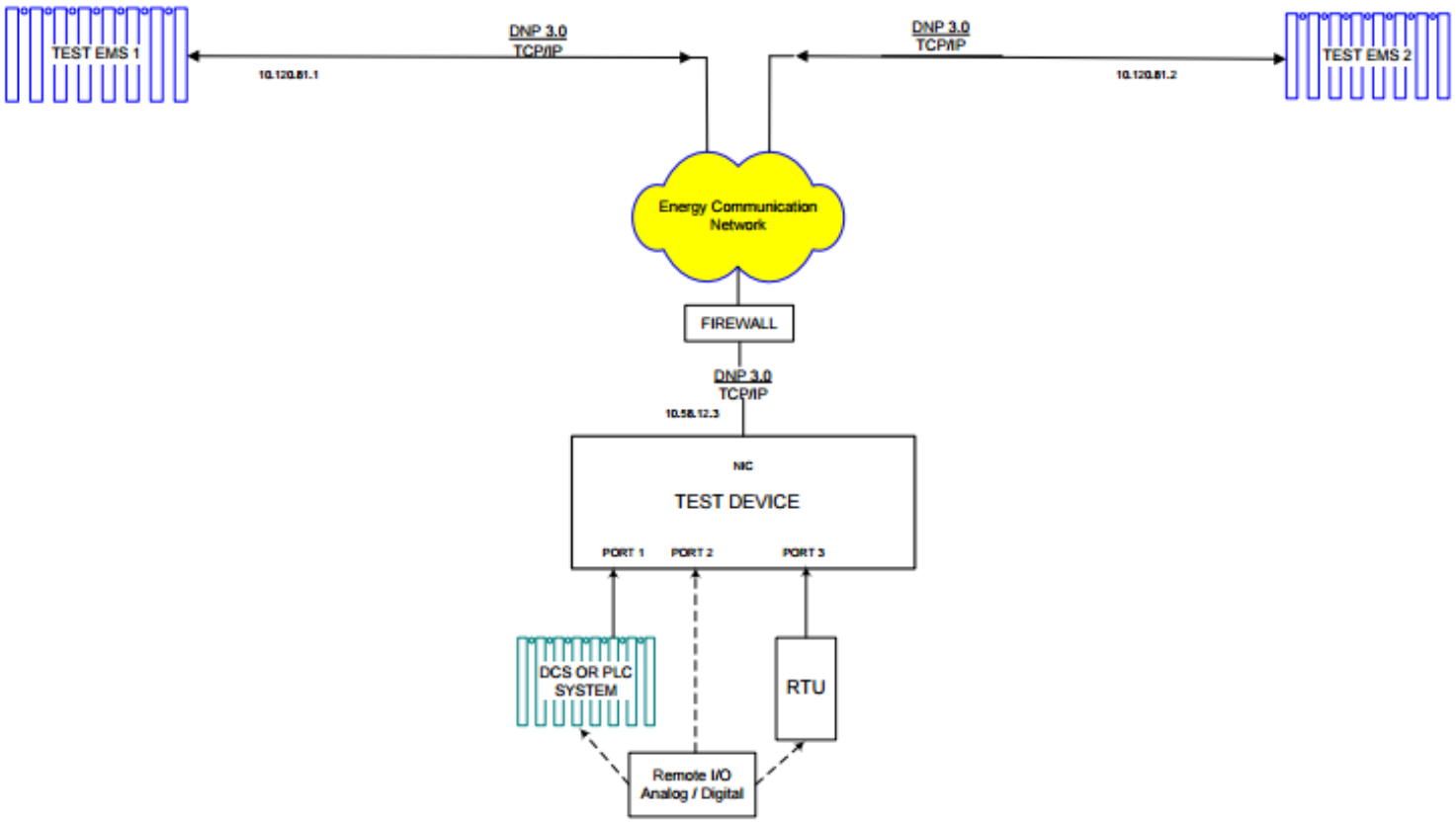
Current ISO Telemetry Security Architecture

Currently, the ISO provides confidentiality for RIG telemetry using digital certificates.

- RIG refers to Remote Intelligence Gateway, a configuration of field devices that provides telemetry data to the ISO SCADA system.
- RIG telemetry is a critical component in AGC.
- Security architecture:
  - The RIG has the server role.
  - The SCADA system has the client role and polls the RIG every four seconds.
  - RIG and SCADA systems mutually authenticate.
  - Protocol is “plain” DNP3 (that is, not DNP3 Secure Authentication).
  - Communications network is MPLS VPN.

Non-Repudiation

There can be no “digital doubt” that the signal from the SCADA system reached its destination.



Forces Driving Change

Under various Renewables Portfolio Standards, electricity markets continue on a path toward regionalization.

Regionalization promises to unlock potential for expanding resource flexibility, transmission capabilities, and clean energy.

Industry expansion must be both nimble and secure.

Customers have requested use of public Internet for telemetry.

Customers have requested an alternative to digital certificates.

The Problem of Scalability

Current methods of securing telemetry lack scalability and are relatively costly to implement or are incomplete.

- PKI does not scale easily.
- IPsec does not scale easily and can be costly.
- Point-to-point links are relatively expensive.
- An MPLS VPN:
  - Does help manage cost;
  - Does provide path protection;
  - Does add bandwidth assurance;
  - But natively provides no encryption services.

NISTIR 7628

NIST Interagency Report 7628 documents numerous cryptography challenges in Smart Grid.

We should not simply assume that traditional PKI is the only approach available to us.

CHAPTER FOUR
CRYPTOGRAPHY AND KEY MANAGEMENT

This chapter identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives. The identified alternatives may be existing standards, methods, or technologies, and their optimal adaptations for the Smart Grid. Where alternatives do not exist, the subgroup has identified gaps where new standards and/or technologies should be developed for the industry.

4.1 SMART GRID CRYPTOGRAPHY AND KEY MANAGEMENT ISSUES

4.1.1 General Constraining Issues

4.1.1.1 Computational Constraints

Some Smart Grid devices, particularly residential meters and in-home devices, may be limited in their computational power and/or ability to store cryptographic materials. The advent of low-cost semiconductors, including low-cost embedded processors with built-in cryptographic capabilities, will, however, ease some such constraints when the supply chain—from manufacturing to deployment to operation—absorbs this technology and aligns it with key management systems for Smart Grid operations. We can expect that most future devices connected to the Smart Grid will have basic cryptographic capabilities, including the ability to support symmetric ciphers for authentication and/or encryption. Public-key cryptography may be supported either in hardware by means of a cryptography co-processor or, as long as it is performed infrequently (i.e., less than once per hour), it can be supported in software. We also note that the use of low-cost hardware with embedded cryptography support is a necessary but not wholly sufficient step toward achieving high availability, integrity, and confidentiality in the Smart Grid. A trustworthy and unencumbered implementation of cryptography that is suitable (both computationally and resource-wise) for deployment in the Smart Grid would benefit all stakeholders in Smart Grid deployments.

4.1.1.2 Channel Bandwidth

The Smart Grid will involve communication over a variety of channels with varying bandwidths.

Business Opportunity

We seek an alternative to PKI and VPNs for securing telemetry.

- Network agnostic.
- Protocol agnostic.
- No requirement to provision digital certificates.
- Equivalent security on public and private networks.
- Low initial and recurring costs.
- Fast provisioning.
- Low customer impact and complexity.
- Automated remote maintenance without reboots.

Reliability Is the First Priority

Can a broadband connection over the public Internet provide the same level of service as a T1 line in an MPLS network?

Link criticality can vary with the telemetry services provided by the link (for example, AGC, Ancillary Services, Energy Only).

Who assumes the risk of a failed link?

Availability and reliability mandates transcend confidentiality, integrity, and authentication requirements.

Proof of Concept

The ISO realized that SDN and WAN Virtualization had potential to replace PKI and VPNs without compromising security.

The ISO is exploring these capabilities through partnership with an SDN vendor that offers additional strong security features.

- Replaces older VPN technologies such as IPsec and MPLS.
- Fractionalized or dispersed packets (foils MITM).
- Rapidly rolling encryption keys over independent paths.
- Interleaving (random rearrangement of packet bits).
- False data (red herring).
- Protocol dispersion (TCP or UDP or both).

WAN Virtualization and SDN

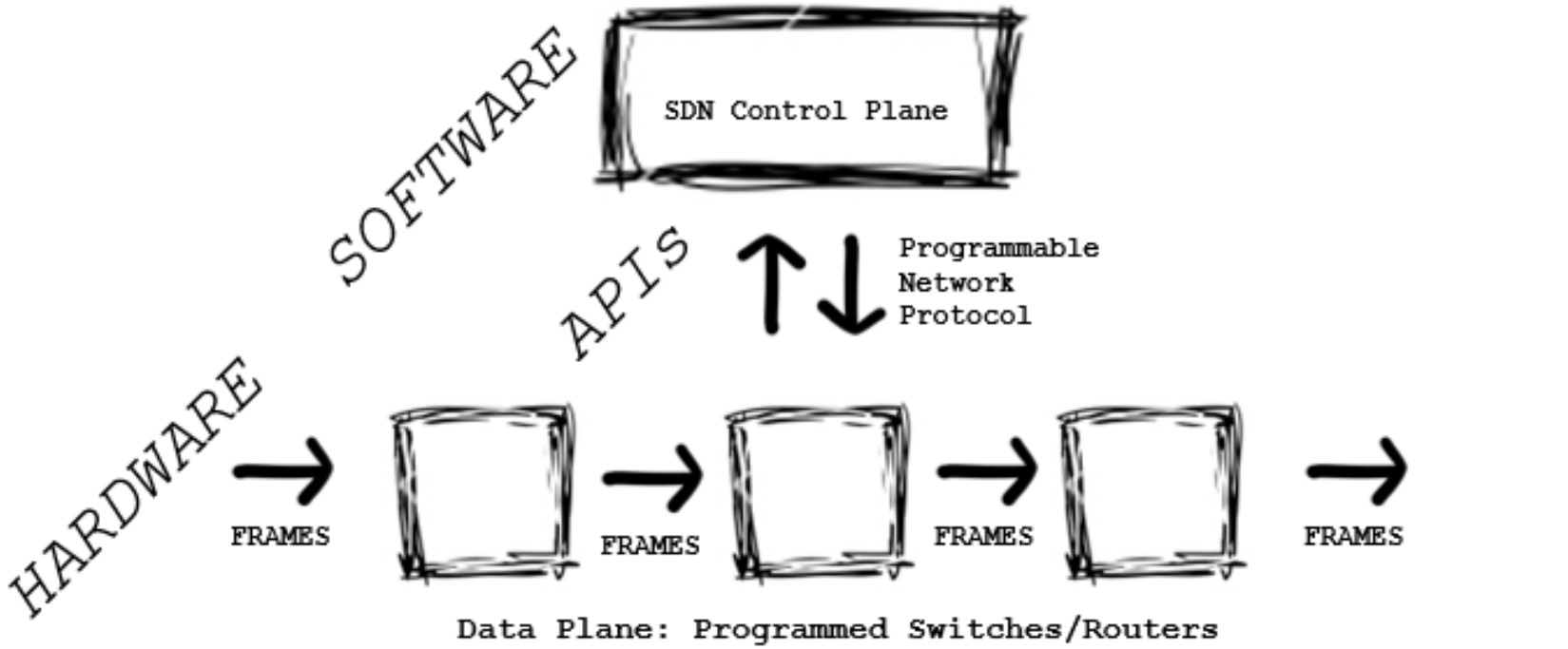
WAN Virtualization

- Aggregates bandwidth over the “middle mile” from multiple links.
- Engineers traffic in real time to “forage” available bandwidth.

SDN

- Decouples data and control functions.
- Centralizes network programmability.
- Provides dynamic administrative control through software.
- Abstracts packet forwarding decisions to software.

Software-Defined Networking



SDN: Path and Bandwidth Optimization

Current Status

Moving toward implementation of SDN for RIGs.

Recognition that SDN is a “middle mile” solution.

Evaluating additional opportunities for retiring SSL/TLS for API communication and Web Services.

Exploring applicability to additional protocols such as ICCP and metering protocols.

Challenges

- “Last mile” reliability questions remain.
- Industry adoption.
- Integration with traditional security tools such as IPS.
- Operational monitoring.
- Fault isolation.
- Training.

Acronyms

- AGC: Automatic Generation Control
- API: Application Program Interface
- DNP3: Distributed Network Protocol Version 3
- FERC: Federal Energy Regulatory Commission
- ICCP: Inter-Control Center Communications Protocol
- IP: Internet Protocol
- IPS: Intrusion Protection System
- IPsec: Internet Protocol Security
- ISO: Independent System Operator
- MITM: Machine in the Middle
- MPLS: Multiprotocol Label Switching
- NERC: North American Electric Reliability Corporation
- NISTIR: National Institute of Standards and Technology Interagency Report
- NREL: National Renewables Energy Lab
- PKI: Public Key Infrastructure
- RIG: Remote Intelligence Gateway
- RTO: Regional Transmission Organization
- SCADA: Supervisory Control and Data Acquisition
- SDN: Software-Defined Networking
- SSL: Secure Sockets Layer
- TCP: Transmission Control Protocol
- TLS: Transport Layer Security
- UDP: User Datagram Protocol
- VPN: Virtual Private Network
- WAN: Wide-Area Network